(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 818 766**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 16724**

(51) Int Cl[7] : G 06 F 9/44, G 06 F 9/445

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 21.12.00.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 28.06.02 Bulletin 02/26.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *BULL CP8 Société anonyme* — FR.

(72) Inventeur(s) : GIRAUD NICOLAS.

(73) Titulaire(s) :

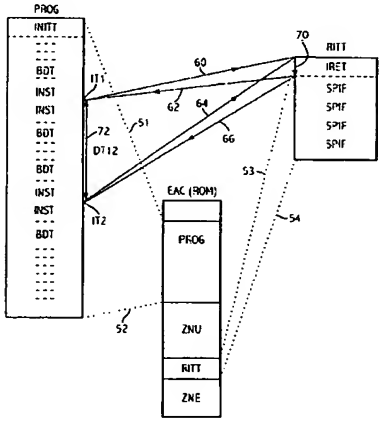
(74) Mandataire(s) : CP8 TECHNOLOGIES.

(54) PROCEDE DE SECURISATION DE L'EXECUTION D'UN PROGRAMME IMPLANTE DANS UN MODULE ELECTRONIQUE A MICROPROCESSEUR, AINSI QUE LE MODULE ELECTRONIQUE ET LA CARTE A MICROCIRCUIT ASSOCIES.

(57) Le procédé de sécurisation de l'exécution d'un programme PROG implanté en ROM dans un module électronique à microprocesseur comporte au moins les étapes suivantes: - on déclenche par intermittence à l'aide d'un décompteur à réarmement automatique inclus dans le module une interruption IT1, IT2 dans l'exécution du programme PROG; et

- on déroute 60, 66 à chaque interruption IT1, IT2 l'exécution du programme vers une routine de gestion de l'interruption RITT comportant comme première instruction l'instruction de retour d'interruption IRET 70 vers le programme 62, 66 au point de déroutage de l'interruption IT1, IT2.

L'invention concerne également un module électronique à microprocesseur adapté pour mettre en oeuvre le procédé ci dessus.



FR 2 818 766 - A1

PROCEDE DE SECURISATION DE l'EXECUTION D'UN PROGRAMME IMPLANTE DANS UN MODULE ELECTRONIQUE A MICROPROCESSEUR, AINSI QUE LE MODULE ELECTRONIQUE ET LA CARTE A MICROCIRCUIT ASSOCIES

La présente invention concerne la sécurisation de modules électroniques comportant au moins un microprocesseur, une mémoire de type ROM/EEPROM contenant au moins un programme à exécuter et des moyens d'entrée/sortie pour communiquer avec l'extérieur. De tels modules sont réalisés le plus souvent sous la forme d'un microcircuit électronique intégré monolithique, ou puce, qui une fois protégé physiquement par tout moyen connu peut être monté sur un objet portatif type carte à puce, carte à microcircuit ou analogue utilisable dans divers domaines, notamment les cartes bancaires et/ou commerciales, la radiotéléphonie mobile, la télévision à péage, la santé et les transports.

D'une façon générale la sécurisation est destinée à accroître la sécurité anti-fraude d'un programme qui comporte un certain nombre d'instructions particulièrement critiques pour la bonne exécution de ce programme, en particulier certaines instructions à caractère opérationnel relatives au déroulement d'une transaction par l'intermédiaire du module électronique et/ou des instructions à caractère sécuritaire propre concernant par exemple l'authentification de l'utilisateur, l'authentification de la transaction et de sa validité, le maintien de la confidentialité des données, le cryptage/décryptage des données.

Si l'utilisation frauduleuse des cartes à puce n'est pas un phénomène nouveau, l'accroissement du volume et de la valeur des transactions sur carte à puce a amené les fraudeurs à utiliser des méthodes et des moyens de plus

en plus sophistiqués. En particulier des attaques par rayonnements brèves et ciblées sur la puce ont pour conséquence de modifier les données et/ou les codes transitant d'une mémoire programme ROM et/ou EEPROM vers le microprocesseur sur le bus interne avec pour résultat l'inexécution ou l'exécution irrégulière de certaines parties du code, par exemple l'exécution d'instructions inopérantes en lieu et place d'une séquence de traitement sécuritaire.

Les parades à base de détecteurs de rayonnement s'avèrent inefficaces du fait de la finesse et la précision des émetteurs de rayonnements utilisés par les fraudeurs d'une part et du fait du risque de perturbation par rayonnement de la séquence logicielle de traitement du capteur d'autre part. Parmi d'autres solutions proposées, notamment dans le cadre de la demande de brevet français n°99.08409 au nom du Demandeur, certaines, comme le contrôle de parité sur le bus, nécessitent des modifications au niveau du dessin et de la conception de la puce elle-même, d'autres, comme l'introduction de drapeaux en RAM, ne font appel qu'à des solutions purement logicielles et de ce fait sont susceptibles d'être contournées par le type même d'attaques qu'elles visent à neutraliser.

La présente invention a pour but de s'assurer de la bonne exécution du code d'instructions contenu en ROM et/ou en EEPROM et qu'aucune attaque par rayonnement n'est en cours et en cas d'attaque d'arrêter l'exécution normalement prévue du programme (l'exécution de la session en cours).

A cette fin l'invention propose un procédé de sécurisation de l'exécution d'un programme implanté en mémoire ROM et/ou EEPROM dans un module électronique à

microprocesseur caractérisé en ce qu'il comporte au moins les étapes suivantes :

- on déclenche par intermittence à l'aide de moyens matériels inclus dans le module une interruption dans l'exécution du programme; et
- on déroute à chaque interruption, à l'aide du microprocesseur, l'exécution du programme vers une routine de gestion de l'interruption comportant comme première instruction ou parmi les premières instructions de la routine l'instruction de retour au programme au point de déroutage.

A chaque interruption provoquée le code programme est dérouté vers une routine de traitement de cette interruption qui prévoit un retour normal au point de déroutage du programme, ce dernier poursuivant alors son exécution. De plus une attaque par rayonnement n'est pas capable d'empêcher le déclenchement d'une interruption par les moyens matériels inclus dans le module. Si cette attaque par rayonnement persiste lors de l'exécution de la routine de traitement de l'interruption provoquée, elle entraînera l'inexécution de l'instruction de retour au programme et de fait empêchera l'exécution correcte de la suite de ce programme.

Le procédé selon l'invention fournit ainsi une parade efficace aux attaques par rayonnement qui est susceptible d'être mise en oeuvre en utilisant des circuits préexistants (sans adaptation matérielle ni modification du dessin ou de la conception de la puce électronique) et des ressources mémoires limitées et qui ne pénalise pas de façon sensible les performances du module électronique.

De préférence la première instruction de la routine de gestion de l'interruption est constituée par

l'instruction de retour au programme au point de déroutage pour revenir au traitement interrompu. En effet il n'est en général pas nécessaire de prévoir de traitement logiciel préalable à l'instruction de retour puisque celui-ci ne sera pas exécuté en cas d'attaque par rayonnement en cours. Ainsi la routine de gestion de l'interruption peut être réduite à seule une instruction de façon à ne pas affecter sensiblement les performances du programme et à ne pas utiliser trop de volume mémoire dans la mémoire ROM/EEPROM.

Selon un mode de réalisation préférentiel de l'invention la routine de gestion de l'interruption est placée en ROM et/ou en EEPROM au dernier emplacement de la mémoire programme ou juste avant une frontière de domaine partagé de façon à sortir de la zone de mémoire programme autorisée lors de l'incrémentation du compteur de programme en cas de non-exécution de l'instruction de retour au programme. Il en résulte une interruption non masquable et un blocage immédiat du microprocesseur perceptible d'emblée par l'utilisateur.

Selon une autre variante intéressante du procédé selon l'invention l'instruction de retour au programme de la routine de gestion de l'interruption est immédiatement suivie en ROM et/ou en EEPROM d'une séquence de positionnement d'un indicateur de fraude en mémoire, notamment en mémoire EEPROM ou analogue, pour avertir d'une attaque frauduleuse passée.

Selon un mode de réalisation préférentiel de l'invention, les moyens matériels comportent un circuit décompteur (timer) à réarmement automatique ou un circuit électronique analogue. Ainsi une exception est levée à chaque fois que le décompteur (également appelé minuteur) arrive à expiration. Cette exception est suivie du

déroutage de code programme vers la routine de traitement de l'interruption décompteur. Le choix d'un décompteur à réarmement automatique comme générateur d'interruption est particulièrement intéressant à plusieurs titres, d'une part les décompteurs à réarmement automatique font partie de l'équipement de base des modules électroniques à microprocesseur, notamment les microcontrôleurs, et d'autre part parce qu'ils s'avèrent assez faciles à mettre en oeuvre du point de vue programmation. En effet on utilise directement l'instruction retour de l'interruption. En conclusion le décompteur à réarmement automatique est le moyen matériel très simple et très fiable pour provoquer une interruption sans intervention logicielle et à intervalles réguliers grâce au réarmement automatique.

Selon une première variante opératoire la valeur d'initialisation du circuit décompteur est rendue variable, notamment à chaque redémarrage du programme (nouvelle session). Avantageusement la variation de la valeur d'initialisation du circuit décompteur comporte au moins un paramètre obtenu à partir d'un générateur de nombres pseudo-aléatoires, sous-ensemble également fréquemment présent dans les microcontrôleurs pour traitements sécurisés. Ainsi le moment où un traitement est interrompu et le contrôle réalisé est rendu variable très difficilement prévisible, voire imprévisible, pour les fraudeurs.

L'invention prévoit à titre optionnel un certain nombre de procédures et/ou caractéristiques complémentaires destinées à encore augmenter l'efficacité de l'invention. Parmi celles-ci on peut citer :

- la répétition dans la suite d'instructions du programme de certaines instructions, notamment d'instructions sécuritaires de façon à augmenter en cas d'attaque les

chances d'interruption au cours de l'exécution de cette séquence d'instructions ;

- l'introduction dans la suite d'instructions du programme d'au moins une boucle de décalage temporel de l'exécution d'instructions avec en option la variation du décalage temporel d'une boucle à une autre et l'introduction d'un paramètre aléatoire dans cette variation par l'intermédiaire d'un générateur de nombres pseudo-aléatoires.

L'invention concerne également des modules électroniques sécurisés comportant chacun au moins un microprocesseur, une mémoire ROM et/ou une mémoire EEPROM comprenant au moins un programme à exécuter, le module étant caractérisé en ce qu'il comporte des moyens matériels adaptés pour déclencher par intermittence une interruption dans l'exécution du programme et en ce que la mémoire ROM et/ou EEPROM comporte une routine de gestion de l'interruption comportant comme première instruction ou parmi les premières instructions de la routine l'instruction de retour au programme au point de déroutage.

Selon une autre variante optionnelle du module de l'invention la routine de gestion de l'interruption est placée en ROM et/ou EEPROM au dernier emplacement de la mémoire programme ou juste avant une frontière de domaine partagé de façon à sortir de la zone de mémoire programme autorisée lors de l'incrémentation du compteur de programme en cas de non-exécution de l'instruction de retour au programme.

Selon une variante optionnelle du module de l'invention l'instruction de retour au programme de la routine de gestion de l'interruption est immédiatement suivie en ROM et/ou en EEPROM d'au moins une séquence de positionnement

d'un indicateur de fraude en mémoire, notamment en mémoire EEPROM ou analogue, l'indicateur étant adapté de façon optionnelle pour avertir d'une attaque frauduleuse passée.

Selon un mode de réalisation préférentiel du module de l'invention les moyens matériels comportent un circuit décompteur à réarmement automatique ou un circuit électronique analogue.

De plus le module comporte des moyens matériels et/ou logiciels pour faire varier la valeur d'initialisation du circuit décompteur, notamment à l'aide d'un générateur de nombres pseudo-aléatoires.

Avantageusement certaines d'instructions, notamment des instructions sécuritaires, sont répétés en mémoire ROM/EEPROM dans la suite d'instructions du programme implanté dans le module selon l'invention.

Tout aussi avantageusement au moins une boucle de décalage temporel de l'exécution de certaines d'instructions est introduite dans la mémoire ROM et/ou EEPROM du module dans la suite d'instructions du programme. En variante le décalage temporel est variable d'une boucle à une autre, notamment à l'aide d'un générateur de nombres pseudo-aléatoires.

L'invention concerne également une carte à microcircuit comportant un module électronique sécurisé tel que défini ci-avant dans ses différentes variantes.

D'autres buts, avantages et caractéristiques de l'invention apparaîtront à la lecture de la description qui va suivre de la mise en oeuvre du procédé selon l'invention et d'un mode de réalisation d'un module

électronique à microprocesseur selon l'invention donnés à titre d'exemple non limitatif en référence aux dessins ci-annexés dans lesquels:

- la figure 1 montre une représentation schématique d'un mode de réalisation d'un module électronique à microprocesseur selon l'invention; et
- la figure 2 montre une représentation schématique de l'espace d'adressage code de la mémoire ROM de la figure 1 accompagné de deux sous-parties de programme plus détaillées, la portion de code à protéger et la routine d'interruption.

Le module électronique monolithique 10 à microprocesseur illustré à la figure 1 selon la présente invention et décrit à titre d'exemple non limitatif comporte d'une façon générale un microprocesseur CPU 11 relié de façon bidirectionnelle par un bus interne 12 à une mémoire vive RAM 14, une mémoire morte ROM 16, une mémoire EEPROM 18 et une interface entrée/sortie I/O 20. Le module 10 comporte également un décompteur TIMER 22 à réarmement automatique et un générateur de nombres pseudo-aléatoires GNPA 24 reliés au bus interne 12.

Comme indiqué ci-après le décompteur 22 et le générateur GPNA 24 sont utilisés dans le cadre de la présente invention pour le déclenchement par intermittence d'interruptions dans l'exécution de certains programmes implantés dans la ROM 16, notamment le programme PROG comportant des instructions dits sécuritaires, telles par exemple des instructions de cryptage/décryptage, des instructions d'authentification d'opérateur ou des instructions de validation de transaction (et repérées par le code INST en figure 2).

A titre d'exemple non limitatif un module selon l'invention est utilisable, en association avec un objet

support pour former une carte à microcircuit, comme carte bancaire ou comme porte-monnaie électronique. En ce qui concerne le cadencement du décompteur 22, celui ci est réduit par rapport à la fréquence de l'horloge par un facteur de division variable selon les modules et en général compris entre 4 et 32, ce qui donne un intervalle minimum entre les déclenchements de deux interruptions successives compris entre 1 et 8 instructions.

La figure 2 illustre l'espace d'adressage code de la mémoire ROM 16 de la figure 1 et intitulé EAC(ROM). Cet espace EAC(ROM) se présente sous la forme d'une séquence de lignes de code (données et constantes comprises) allant de l'adresse la plus basse en haut de colonne à l'adresse la plus haute en bas de colonne. Cet espace EAC(ROM) est partagé en domaines contenant notamment des programmes, tels le programme PROG, et des routines, telle la routine RITT, routine de gestion de l'interruption déclenchée par décompteur. L'espace EAC(ROM) comporte également en bas de colonne une zone sans mémoire ou une zone de mémoire non exécutable ZNE, la zone mémoire exécutable encore disponible et non utilisée étant dénommée ZNU. Selon une caractéristique optionnelle mais très intéressante de l'invention exposée ci-après, la routine RITT est implantée juste avant la zone ZNE.

La figure 2 montre également une illustration en colonne agrandie du programme PROG et une illustration en colonne agrandie de la routine de gestion de l'interruption RITT avec en pointillé les segments de correspondance des adresses de tête et de queue des sous parties logicielles correspondants, les segments 51 et 52 pour la colonne PROG et les segments 53 et 54 pour la colonne RITT.

Le programme PROG comporte en tête un jeu d'instructions INITT concernant la configuration et l'initialisation du décompteur à réarmement automatique 22 y compris la gestion de l'utilisation du générateur GNPA 24 pour la détermination de la valeur d'initialisation du compteur à défilement décroissant intégré dans le décompteur 22. Les instructions INITT sont suivies des lignes du programme PROG proprement dit (chaque ligne indifférenciée étant représentée par 3 tirets au centre de la ligne). Tel que représenté sur la figure 2 à titre d'exemple le programme PROG comporte au moins deux instructions INST à sécuriser. Ces instructions peuvent être identiques (répétition pour que l'instruction ait de bonnes chances d'être exécutée avec une interruption de contrôle) ou distinctes en cas de multiplicité d'instructions (authentification d'opérateur en début de transaction et de validation de transaction à la fin). Les instructions INST sont encadrées par des boucles à décalage temporel BDT destinées à décaler d'une durée aléatoire l'exécution de la prochaine instruction INST.

La routine RITT correspondant à la routine de traitement d'interruption décompteur comporte comme première instruction, l'instruction IRET de retour d'interruption au point de déroutage du programme PROG. De façon optionnelle l'instruction IRET est suivie d'une ou plusieurs séquences de positionnement en mémoire d'un indicateur de fraude SPIF en l'espèce dans la mémoire EEPROM 18. Au positionnement d'un indicateur de fraude proprement dit, est associée une procédure d'interdiction du fonctionnement opérationnel ultérieur du module électronique.

L'exécution du programme PROG s'effectue de la façon suivante en défilant la séquence d'instructions de la colonne PROG et commence par le chargement dans le

compteur du décompteur 22 de sa valeur initiale, une valeur préétablie et éventuellement déjà modifiée par prise en compte d'un paramètre de variation obtenu à partir du générateur GNPA 24. Au fur et à mesure de l'exécution du programme PROG, la valeur instantanée du compteur/décompteur du décompteur 22 décroît jusqu'à expiration et atteindre la valeur zéro pendant l'exécution d'une instruction de PROG, par exemple la première instruction INST de la colonne PROG. Il s'ensuit la levée d'une exception et, après la fin de l'exécution de l'instruction en cours, le déroutage au point IT1 selon la flèche 60 du code programme vers la routine de traitement de l'interruption décompteur représentée par la colonne RITT, l'instruction suivante à exécuter dans le registre « compteur programme » du microprocesseur 11 étant la première instruction de la colonne RITT, c'est à dire l'instruction IRET de retour d'interruption au point IT1 selon la flèche 62. En cas d'absence d'attaque par rayonnement l'instruction IRET est exécutée normalement selon la flèche 70 comme le retour vers le point IT1 selon la flèche 62. Le compteur/décompteur du décompteur est alors réinitialisé de façon automatique et correspondant à l'intervalle de temps d'exécution DT12 du programme PROG passé entre le point IT1 (instant « retour ») et le point IT2 correspondant à la seconde interruption (instant « déroutage ») et représenté sur la colonne PROG par la double flèche 72. En l'absence d'attaque par rayonnement lors de la seconde interruption IT2 la procédure décrite ci-avant se répète avec déroutage vers la routine RITT selon la flèche 64, l'exécution normale selon 70 de l'instruction IRET de cette routine et le retour au point IT2 selon la flèche 66.

A titre de variante il est possible d'utiliser un compteur/décompteur à réarmement non automatique à

commande logicielle intégrée à la routine RITT. Il est ainsi possible de donner au compteur/décompteur une nouvelle valeur initiale différente de la précédente valeur initiale, éventuellement en ajoutant avec une composante aléatoire à l'aide du générateur GNPA 24. Cette caractéristique présente de l'intérêt notamment si l'on recherche à augmenter ou à réduire la fréquence des interruptions selon l'état d'avancement de l'exécution du programme.

D'une façon générale la durée d'une attaque par rayonnement recouvre environ le temps d'exécution de plusieurs instructions de code programme que celles-ci soient normalement exécutées ou exécutées de façon inopérante du fait de l'altération des codes programme en transit sur le bus interne 12 lors d'une attaque par rayonnement. Ainsi les intervalles variables entre deux interruptions sont distants d'environ une centaine d'instructions, étant entendu qu'un rapprochement d'intervalles entre interruptions est toujours possible au cours de l'exécution d'un programme code autour des instructions à sécuriser (dans la limite des possibilités de déclenchement du décompteur utilisé) en prenant garde de ne pas allonger sensiblement le temps d'exécution du programme concerné.

En cas d'attaque par rayonnement en cours au moment où la valeur du compteur/décompteur du décompteur 22 atteint la valeur zéro, la procédure d'interruption sur décompteur entièrement gérée par un support matériel insensible à ce type d'attaque (le microprocesseur 11) s'exécutera normalement avec déroutage selon la flèche 60 vers la routine RITT. Par contre l'attaque par rayonnement empêchera l'exécution de l'instruction logicielle de retour d'interruption IRET 70 au point de déroutage IT1 et l'exécution du programme PROG ne pourra pas reprendre,

le compteur programme du microprocesseur 11 gardant comme instruction suivante la première instruction SPIF. Le parcours sans effet de la routine RITT se continue jusqu'à la dernière instruction SPIF, étant fait remarquer qu'en cas d'arrêt de l'attaque avant la dernière instruction SPIF, au moins une séquence de positionnement d'un indicateur de fraude est exécutée selon l'instruction SPIF pour signaler à l'OS (de l'anglais « Operating System » ou système d'exploitation) du microprocesseur l'attaque par rayonnement passée et provoquer l'interdiction par l'OS de la poursuite de la session en cours d'exécution.

Du fait de la position particulière de la routine RITT en ROM 16 au dernier emplacement de la mémoire programme (ou juste avant une frontière de domaine partagé) l'incrémentation du compteur de programme à la fin de la routine RITT provoquera une sortie de la zone de mémoire programme autorisée pour entrer dans la zone de mémoire non exécutable ZNE. Ceci aura pour effet de déclencher une interruption non masquable et un traitement en vue de l'interdiction de la poursuite de la session en cours d'exécution.

On notera pour finir que la mise en oeuvre du procédé selon l'invention est assez simple et peu coûteuse en ressources et en temps. Elle utilise le décompteur à réarmement automatique présent dans la puce et l'interruption associée. Seul est nécessaire l'ajout du code d'initialisation en début de session de programme et de la routine de gestion de l'interruption, routine qui peut être réduite à une seule instruction. Le temps d'exécution consommé par la mise en oeuvre du procédé correspond à l'initialisation du décompteur en début de session et à l'exécution de l'instruction de retour d'interruption à chaque interruption. Le procédé selon

l'invention peut être utilisé sur les portions les plus sensibles d'un programme ou être étendu à la protection de l'intégralité du code programme sans véritablement pénaliser les performances de celui-ci en volume mémoire et en temps d'exécution.

Le module 10 avec son programme sécurisé selon l'invention tels que présenté ci-avant est monté sur un support approprié pour réaliser par exemple une carte à microcircuit utilisable dans divers domaines, notamment les cartes bancaires et/ou commerciales, la radiotéléphonie mobile, la télévision à péage, la santé et les transports.

L'invention n'est pas limitée à l'utilisation de modules électroniques à décompteur à réarmement automatique mais s'applique également aux modules électroniques dont l'architecture et les moyens matériels sont susceptibles de déclencher des interruptions provoquées, et notamment à des modules électroniques incorporant des circuits à base de temps analogues aux circuits décompteurs à réarmement automatique ou à réarmement logiciel, par exemple des circuits basés tant sur le comptage/décomptage d'impulsions d'horloge que sur le comptage du nombre d'instructions ou de lignes d'instructions effectivement exécutées.

REVENDICATIONS:

1. Procédé de sécurisation de l'exécution d'un programme implanté en mémoire ROM (16) et/ou EEPROM (18) dans un module électronique (10) à microprocesseur (11) caractérisé en ce qu'il comporte au moins les étapes suivantes :
- on déclenche par intermittence à l'aide de moyens matériels (11) inclus dans le module (10) une interruption dans l'exécution du programme ; et
- on déroute à chaque interruption, à l'aide du microprocesseur, l'exécution du programme vers une routine de gestion de l'interruption comportant comme première instruction ou parmi les premières instructions de la routine l'instruction de retour au programme au point de déroutage.

2. Procédé selon la revendication 1 caractérisé en ce que la routine de gestion de l'interruption est placée en ROM (16) et/ou en EEPROM (18) au dernier emplacement de la mémoire programme ou juste avant une frontière de domaine partagé de façon à sortir de la zone de mémoire programme autorisée lors de l'incrémentation du compteur de programme en cas de non-exécution de l'instruction de retour au programme.

3. Procédé selon la revendication 1 caractérisé en ce que l'instruction de retour au programme de la routine de gestion de l'interruption est immédiatement suivie en ROM (16) et/ou en EEPROM (18) d'une séquence de positionnement d'un indicateur de fraude en mémoire, notamment en mémoire EEPROM (18) ou analogue, pour avertir d'une attaque frauduleuse passée.

4. Procédé selon la revendication 1 caractérisé en ce que lesdits moyens matériels comportent un circuit décompteur

à réarmement automatique (22) ou un circuit électronique analogue.

5. Procédé selon la revendication 4 caractérisé en ce que la valeur d'initialisation du circuit décompteur (22) est variable.

6. Procédé selon la revendication 5 caractérisé en ce que la variation de la valeur d'initialisation du circuit décompteur (22) comporte au moins un paramètre obtenu à partir d'un générateur de nombres pseudo-aléatoires (24).

7. Procédé selon la revendication 1 caractérisé en ce que certaines instructions, notamment des instructions sécuritaires, sont répétées dans la suite d'instructions du programme.

8. Procédé selon la revendication 1 caractérisé en ce qu'au moins une boucle de décalage temporel de l'exécution d'instructions est introduite dans la suite d'instructions du programme.

9. Procédé selon la revendication 8 caractérisé en ce que le décalage temporel est variable d'une boucle à une autre.

10. Procédé selon la revendication 9 caractérisé en ce que la variation du décalage temporel comporte au moins un paramètre obtenu à partir d'un générateur de nombres pseudo-aléatoires (24).

11. Module électronique (10) comportant au moins un microprocesseur (11) et une mémoire ROM (16) et/ou une mémoire EEPROM (18) comprenant au moins un programme à exécuter, le module étant caractérisé en ce qu'il comporte des moyens matériels (22) adaptés pour

déclencher par intermittence une interruption dans l'exécution du programme et en ce que ladite mémoire ROM (16) et/ou EEPROM (18) comporte une routine de gestion de l'interruption comportant comme première instruction ou parmi les premières instructions de la routine l'instruction de retour au programme au point de déroutage.

12. Module (10) selon la revendication 11 caractérisé en ce que lesdits moyens matériels comportent un circuit décompteur du type à réarmement automatique (22) ou un circuit électronique analogue.

13. Module (10) selon la revendication 14 caractérisé en ce qu'il comporte des moyens matériels et/ou logiciels pour faire varier la valeur d'initialisation du circuit décompteur, notamment à l'aide d'un générateur de nombres pseudo-aléatoires (24).

14. Carte à microcircuit caractérisée en qu'elle comporte un module électronique selon la revendication 11.

FIG.1

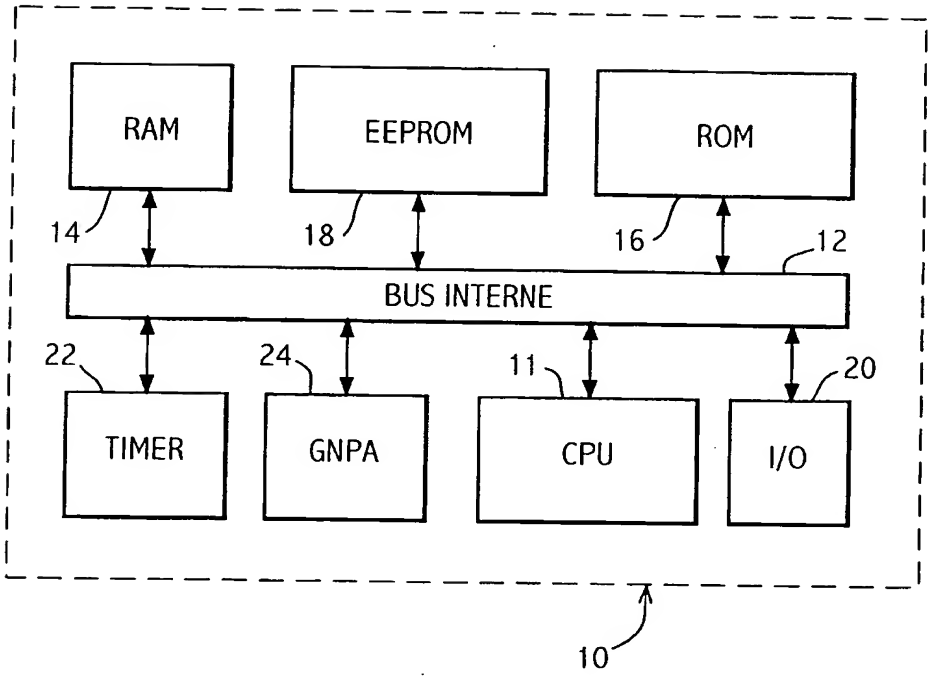
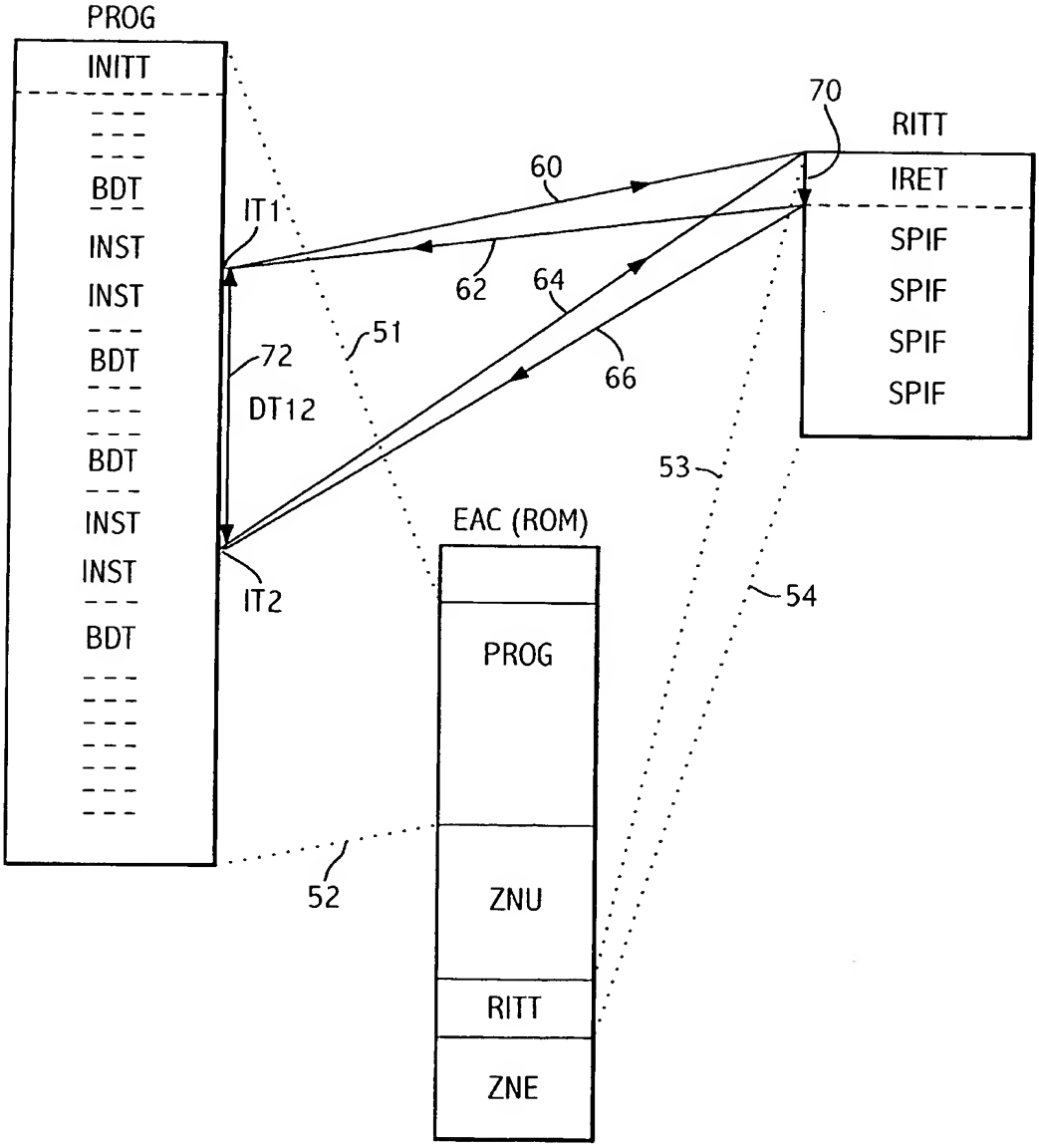

RAM
EEPROM
ROM
14
18
16
12
BUS INTERNE
22
24
11
20
TIMER
GNPA
CPU
I/O
10

FIG.2


PROG
INITT
BDT
INST
INST
BDT
BDT
INST
INST
BDT
IT1
IT2
72
DT12
51
60
62
64
66
70
RITT
IRET
SPIF
SPIF
SPIF
SPIF
53
54
EAC (ROM)
PROG
ZNU
RITT
ZNE
52

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2818766

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 600597
FR 0016724

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X A	WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 septembre 1997 (1997-09-12) * page 5, ligne 31 - page 14, ligne 15 * * figures 1,2,8 *	1,4-14 2	G06F9/44 G06F9/445
X A	FR 2 764 716 A (BULL CP8) 18 décembre 1998 (1998-12-18) * abrégé * * page 1, ligne 6 - ligne 21 * * page 7, ligne 20 - page 12, ligne 7 * * figures 1,2A-2D *	1,11,14 2,4,12	
A	WO 00 23866 A (NACCACHE DAVID ;ANGUITA PHILIPPE (FR); GEMPLUS CARD INT (FR)) 27 avril 2000 (2000-04-27) * abrégé * * page 2, ligne 5 - page 6, ligne 16 *	1,2,4-14	
A	US 5 465 349 A (GERONIMI FRANCOIS ET AL) 7 novembre 1995 (1995-11-07) * abrégé * * colonne 3, ligne 41 - ligne 58 *	1,3,11, 14	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G06F
G06K
G11C

Date d'achèvement de la recherche: 21 septembre 2001

Examinateur: Jacobs, P

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 12.99 (P04C14)